

The United States House of Representatives Information Security Publication

**Guidelines for Determining Information Sensitivity**

---

**Introduction**

This guideline assists U.S. House of Representatives (House) Members, Offices, Committees, and staff in determining the level of sensitivity of the information processed or stored on their computer systems.

House computer systems process and store a variety of information. Some House information is freely accessible to the public while other information is confidential and must be protected accordingly. Confidential information falls into one of two categories:

- Confidential Business Information: any procurement, proprietary, financial, information technology-related, commercial, or information afforded protection from disclosure by statutes applicable to the House (e.g., phone credit card number, network infrastructure information, contract proposals, etc.).
- Confidential House Information: personal information about individuals contained in any collection of records on individuals from which information is retrieved by the individual's name or other personal identifiers such as Social Security Number (e.g., medical history, work performance, etc.).

Any office using computer applications to store or process information should complete the following questionnaire to determine if the information is confidential. If the answer to any question in any category below is "yes" the information should be considered confidential and must be protected accordingly.

**Personnel Information**

Does the information relate to House employees:

Yes\_\_\_No\_\_\_ Payroll data?

Yes\_\_\_No\_\_\_ Fringe benefits information?

Yes\_\_\_No\_\_\_ Terms of employment (including performance/disciplinary records)?

Yes\_\_\_No\_\_\_ Academic/educational history?

Yes\_\_\_No\_\_\_ Arrest/criminal investigation history?

Yes\_\_\_No\_\_\_ Employment history (general and security/clearance information)?

Yes\_\_\_No\_\_\_ Biographical history?

Yes\_\_\_No\_\_\_ Social security information?

Yes\_\_\_No\_\_\_ Symbolic identification codes (e.g., passwords, user IDs)?  
Yes\_\_\_No\_\_\_ A personnel profile (to include home address or phone number)?  
Yes\_\_\_No\_\_\_ Medical history?  
Yes\_\_\_No\_\_\_ Is the information related to internal personnel rules and practices of the House?

### **Financial/Budgetary Information**

Yes\_\_\_No\_\_\_ Does the information contain contract bidding information?  
Yes\_\_\_No\_\_\_ Does the information contain site-operating expenditures? (i.e., phone bills, office lease)?  
Yes\_\_\_No\_\_\_ Does the information address security expenditures? (i.e., firewalls, alarm systems)?

### **Mission-Essential Information**

Yes\_\_\_No\_\_\_ Would the loss of this information adversely impact the ability of the House or office to perform its mission?  
Yes\_\_\_No\_\_\_ Would the loss or unavailability of this information adversely impact the House or office?  
Yes\_\_\_No\_\_\_ Does the application or system used to process this information support other systems or an operation which must be continued to completion without interruption?  
Yes\_\_\_No\_\_\_ Is the application or system that processes this information solely dependent on automated means for execution?  
Yes\_\_\_No\_\_\_ Is the information necessary to assure the continuity of essential House activities during and following national emergency conditions?  
Yes\_\_\_No\_\_\_ Would the inappropriate disclosure of information adversely reflect on the credibility of the House or office?

### **Information Technology and Information Security-Related Information**

Yes\_\_\_No\_\_\_ Does the information pertain to the occurrence or reporting of a theft, intrusion, unauthorized access, viruses, or other misuse or abuse of House resources?  
Yes\_\_\_No\_\_\_ Does the information relate to risk or vulnerability assessments that identify weaknesses in House information systems resources that may be exploited?  
Yes\_\_\_No\_\_\_ Does the information identify House networks' components, security features, access logons, or passwords?  
Yes\_\_\_No\_\_\_ Does the information relate to investigation records, techniques, or procedures compiled for law enforcement purposes or a national security intelligence investigation?

**Legislative Information** *(Note: Information relating to statements made to the press, press clippings, newspaper articles, television interviews or coverage, or other statements or documents published outside of the House are not confidential.)*

Yes\_\_\_No\_\_\_ Does the information relate to specific legislative action taken or considered by the office? This includes drafts of bills, research, and other preparatory information.

Yes\_\_\_No\_\_\_ Does the information relate to statements made on the floor of the House by a Member? This includes drafts of such statements, research, and other preparatory information.

Yes\_\_\_No\_\_\_ Does the information relate to a specific congressional hearing or related investigations, witness interviews, or other preparatory work for that hearing?

Yes\_\_\_No\_\_\_ Was the information provided to the House in confidence or with restrictions on its use (i.e., trade secrets, commercial or financial information) from an individual, private entity, or state or federal entity?

Yes\_\_\_No\_\_\_ Does the information consist of intra-House or inter-agency memoranda, letters, or other communications?

### **Constituent Information**

Yes\_\_\_No\_\_\_ Does the information relate to identifiable constituents who provided information to the office in confidence or with restrictions on its use?

Yes\_\_\_No\_\_\_ Does the information provide identifying characteristics about constituents (i.e., names, social security numbers, addresses, telephone numbers, etc.)?

Yes\_\_\_No\_\_\_ Does the information consist of intra-House or inter-agency memoranda, letters, or other communications relating to a constituent?

Yes\_\_\_No\_\_\_ Was the information provided to the House in confidence or with restrictions on its use (i.e., trade secrets, commercial or financial information) from a constituent?

Information designated as confidential should be protected in accordance with the following guidelines.

- Do not store or transmit confidential information on any public access system, including e-mail and the Internet, without protective measures such as encryption.
- Do not allow unauthorized personnel access to facilities and resources that store or process confidential information.
- Dispose of media (e.g., diskettes, disk drives, etc.) in accordance with approved procedures.
- Do not leave paper copies of confidential information unattended.

Observance of these guidelines will ensure House confidential information is protected at all times and in all forms. Questions concerning the above questionnaire or recommended safeguards should be directed to the House Information Resources Information Systems Security Office.